

CYBER SCAMMERS TARGET B.C.

New poll shows most don't protect their digital devices, making B.C. a hot hunting ground for cyber criminals

The Province | 30 Mar 2015

GORDON MCINTYRE | THE PROVINCE

gordmcintyre@theprovince.com twitter.com/gordmcintyre

CYBER SCAMMERS TARGET B.C.



As the 11th annual Fraud Prevention Month winds down, The Province, the accounting firm MNP and the market research firm Mustel Group polled British Columbians about the prevalence and risk of cyber fraud. Among other things, the survey found that about half of B.C. residents feel the risk of financial loss due to computer crime is low; twice as many people say a home or apartment break-in is more likely than loss or theft from a computer; 87 per cent conduct at least some banking online, but 40 per cent do not use secure Wi-Fi to do so; and, stunningly, just three per cent change their passwords regularly. The online survey of 400 residents, undertaken between Feb. 24 and March 9, has a margin of error of plus/minus five per cent at a 95 per cent level of confidence. Those polled were B.C. adults 18 years or older, using Mustel Group's randomly-recruited panel.

B.C. is ripe for the picking when it comes to cyber fraud, especially given that only three per cent of us regularly change the passwords on our various digital devices.

Further, half the population doesn't even take such preventive measures as installing brand-name anti-virus or anti-malware software, according to a recent poll.

And half of British Columbians fail to set up their devices to lock automatically, the survey, undertaken by The Province, accounting firm MNP and market research firm Mustel Group, discovered.

"Since people perceive the risk of cybercrime as low, limited precautions are being taken, ultimately making people even more vulnerable," Evi Mustel said.

Another survey finding: One-third (36 per cent) of cyber-fraud victims did not recover their loss.

"In addition, I believe there is a false sense of security that the credit card companies or banks will cover the losses," Mustel said.

Fraud has been around at least since humankind started writing things down.

While the medium for carrying out fraud has changed over time, the message stays the same, a forensic accountant at MNP said.

"When it comes to fraud, the message has always been the same," said Pat McParland, senior manager of MNP's investigative and forensic services group. "It's 'have I got a deal for you!'" "The message is the same, but what changes is the medium or means by which fraudsters do it.

"And the cyber world we live in has really changed how fraud occurs."

Cyber crime — generally speaking, fraud or identity theft involving the Internet — has soared, according to Vancouver police.

In 2006, the year VPD started tracking the number of cyber crimes reported, there were 39 incidences. In 2007, there were 29. Last year, the number was 426. And consider: According to the MNP/Mustel survey, only one in five file a police report.

"The Internet is becoming a more and more commonplace method of conducting business and doing research," said Sgt. Tony Cavezza of VPD's financial crime unit.

"It stands to reason that crimes related to it are going to increase.

"You see more of it everywhere and it's very difficult to keep up with it."

One of the most-employed frauds is the romance scam.

Nationwide, Canadians reported losing \$14 million to romance fraud schemes in 2014, according to the Canadian Anti-Fraud Centre, and police believe a lot more romance scams are not reported due to embarrassment.

It's the most common cyber scam in Vancouver, Cavezza said.

Typically, scammers steal photos and use dating sites and social media to lure victims into sending money overseas.

They take the time to develop a relationship, gaining the victim's trust.

They may also offer demonstrations of endearment, such as sending flowers or presents. Then, they want to visit. But, oh, wait! An emergency has come up or a family member needs money urgently; unforeseen fees arise at the last minute, they need money for exit visas, travel permits, whatever. Just send cash immediately! "Please, please do not give money to someone you've never met," Cavezza said. "And even if you have met them in person, get as much information as you can."

B.C. also attracts cyber fraudsters because of its sizable retirement community, said Jacklyn Davies, who leads MNP's investigative and forensic services group.

"They're generally less sophisticated when it comes to computers and devices, they're less likely to employ security such as passwords, they're more trusting."

More likely, say, to believe it's their grandchild emailing from Thailand to say he or she is in trouble and needs money, and not some crook in Nigeria.

Younger people, on the other hand, see cyber crime as something inevitable, far more than do older people, according to the survey.

"It's a sort of cost-of-doing-business attitude with younger people," Davies said.

"Plus, they don't have the money older people do."